United States District Court

for the
Western District of New York

UNITED STATES DISTRICT COURT
FILED
NOV 29 2017
MARY C. LOEWENGUTH, CLERK
WESTERN DISTRICT OF NY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

INFORMATION ASSOCIATED WITH APPLE ID richwilbern@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.

Case No. 17-MJ- 670

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: **INFORMATION ASSOCIATED WITH APPLE ID richwilbern@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC. , as more particularly described in Attachment A,**

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*: ***See* Attachment B for the Items to be Seized, all of which are fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2113(a), 2113(e), 2, 924(c)(1)(A)(iii) and (j)(1), and 922(g), all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of **Title 18, United States Code, Sections 2113(a), 2113(e), 2, 924(c)(1)(A)(iii) and (j)(1), and 922(g).**

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew Jasie, NYSP, Task Force Officer
Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.
Date: November 29, 2017

Judge's signature

City and state: Rochester, New York

HONORABLE JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF:

INFORMATION ASSOCIATED WITH APPLE ID **richwilbern@gmail.com** THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.

17-

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF MONROE) SS:
CITY OF ROCHESTER)

I, Andrew Jasie, a Task Force Officer with the Federal Bureau of Investigation, United States Department of Justice, having been first duly sworn, deposes and says:

1. I am a Task Force Officer with the Federal Bureau of Investigation (FBI). As such, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

2. Prior to becoming a Task Force Officer with the FBI, I have been employed by the New York State Police for 17 years. I have been an investigator with the New York State Police for the last 12 years. During that time, I have participated in investigations involving homicide, bank robbery, drug trafficking, fugitives, and Hobbs Act robbery. In addition, I have had the opportunity to work with other FBI agents and other law enforcement agents

and officers of varying experience levels, who have also investigated homicides, drug trafficking networks, fugitives, and robbery cases. My investigative experience detailed herein, and the experience of other law enforcement agents who are participating in this investigation, serve as the basis for the opinions and conclusions set forth herein.

SUBJECT VIOLATIONS

3. Based on the facts set forth in this affidavit, there is probable cause to believe that on or about August 12, 2003, in the Town of Webster, Western District of New York, the defendant, RICHARD LEON WILBERN, by force, violence and intimidation, did take from the person and presence of another, money, namely, in excess of $10,000 in United States currency, belonging to and in the care, custody, control, management and possession of the Xerox Federal Credit Union, a federal credit union whose deposits were then insured by the National Credit Union Administration Board, and in committing the offense, or in avoiding or attempting to avoid apprehension, the defendant did kill another person, to wit, Raymond Batzel, all in violation of Title 18, United States Code, Sections 2113(a), 2113(e); and, that on or about August 12, 2003, in the Town of Webster, Western District of New York, the defendant, RICHARD LEON WILBERN, during and in relation to a crime of violence for which he may be prosecuted in a court of the United States, that is, a violation of Title 18, United States Code, Sections 2113(a) and (e), as set forth in above, the allegations of which are incorporated herein by reference, did knowingly use, carry and discharge, and in furtherance of such crime, did knowingly and unlawfully possess and discharge, a firearm,

and in the course of a violation of this section, caused the death of a person, to wit, Raymond Batzel, through the use of that firearm, all in violation of Title 18, United States Code, Sections 924(c)(1)(A)(iii) and (j)(1) (collectively, the "Subject Violations").

4. I further submit there is probable cause to believe that on or about September 27, 2016, at 23 Tubman Way, Rochester, New York, Richard Wilbern, a previously convicted felon, was in possession of four firearms in violation of Title 18, United States Code, Section 922(g).

5. Because this affidavit is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included each and every fact known to me through my participation in this investigation.

PURPOSE OF AFFIDAVIT

6. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **Apple Inc**. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with Apple ID "**richwilbern@gmail.com**", that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by

the government is described in the following paragraphs and more particularly in Attachments A and B.

7. Based on the facts as set forth in this affidavit, there is probable cause to believe that the property described in Attachment A contains records, fruits, instrumentalities, and evidence of a crime, to wit, violations of Title 18, United States Code, Sections 2113(a), 2113(e) and 2 (credit union robbery, resulting in death), and that he committed a violation of Title 18, United States Code, Sections 924(c)(1)(A)(iii) and (j)(1) (possession and discharge of a firearm in furtherance of a crime of violence, resulting in death), as well as a violation of in violation of Title 18, United States Code, Section 922(g), as more particularly described in Attachment B.

FACTUAL BACKGROUND

8. The Federal Bureau of Investigation, the Webster Police Department, the Monroe County Sheriff's Office, the New York State Police, the Rochester Police Department and the United States Marshals Service have been engaged in an ongoing investigation into the armed credit union robbery/homicide that occurred on August 12, 2003 at the Xerox Federal Credit Union (XFCU), located in Building 304 on the Xerox Corporation campus at 800 Phillips Road, Webster, Western District of New York. In August 2003, the Xerox Federal Credit Union was a federal credit union whose deposits were then insured by the National Credit Union Administration Board.

9. On that date, at approximately 9:45 a.m., a black male (hereinafter referred to as the "Subject") entered the Xerox Federal Credit Union. Witnesses described the Subject as wearing a dark blue nylon jacket with the letters "FBI" written in yellow on the sleeve and back of the jacket. He wore gloves, sunglasses and a poorly fitting wig. The Subject was also carrying a large, rectangular briefcase and a green and gray-colored umbrella. The Subject also had what appeared to be a United States Marshals badge hanging on a chain around his neck. The Subject proceeded into the interior of the credit union and entered a cubicle occupied by a female XFCU employee.

10. Once inside the cubicle, the Subject sat in a chair across the desk from the employee. He placed the umbrella he was carrying upon the female employee's desk. The Subject maintained the large briefcase near his feet. The Subject then explained to the employee, in sum and substance, that he was present to conduct a security assessment and to "stage" a robbery. After additional conversation with the employee, the Subject then removed two firearms from the briefcase. One firearm was described as a handgun and the other as a sawed-off shotgun or sawed-off rifle. The Subject also removed a bag and instructed the employee to fill a bag with money from behind the teller counter. The employee complied with the demands and proceeded to the counter to get the money. As the employee walked to the counter, the Subject stood in the doorway of the female employee's cubicle.

11. Shortly thereafter, the Subject began to lay employees and customers down on the floor. While doing so, the Subject confronted Raymond Batzel, a customer of the credit union. According to bank records and surveillance video, Batzel had just concluded a

banking transaction with the teller at 9:45 a.m. After a very brief verbal altercation with Batzel, the Subject raised a firearm and shot Batzel in the neck, resulting in his death. As the Subject shot Batzel, a second customer had entered the credit union and upon witnessing the shooting of Batzel, attempted to turn and run back outside. The Subject shot the customer in the back as he fled. The customer managed to flee the credit union and was later treated for his injuries.

12. After shooting both customers, the Subject quickly returned to the teller counter area and, while holding the firearm in the air, told credit union employees to fill the bag with cash. The Subject then took the money and the briefcase and quickly fled the credit union. However, the Subject failed to retrieve the umbrella that he initially brought into the credit union. The umbrella was located by law enforcement still lying on the employee's desk. It was thereafter secured and placed into evidence.

2016 FBI PRESS CONFERENCE

13. On March 21, 2016, law enforcement held a press conference at the FBI offices located in Rochester in an effort to elicit additional leads in this investigation. Information was released related to the crime details, as well as enhanced photographs of the Subject who had committed the robbery. Anyone with information was asked to call a dedicated hotline.

14. Shortly thereafter, a concerned citizen (hereinafter referred to as "Citizen") contacted the Federal Bureau of Investigation with material and relevant information. Upon personally interviewing the Citizen, the Citizen stated, among other items of information, and

in sum and substance, that the perpetrator of the crime was likely a former Xerox employee named Richard Wilbern. The Citizen indicated that Wilbern worked for Xerox prior to the robbery but had been fired by the company. The Citizen stated that he/she recognized Wilbern's face from the photos. The Citizen stated that he/she worked at Xerox at a time when Wilbern was also employed there and had significant interaction with him. The Citizen recalled that while Wilbern worked at Xerox, Wilbern filed a federal lawsuit against the company because Wilbern felt that he was treated unfairly and discriminated against based upon his race. Wilbern made comments to the Citizen during the pendency of the lawsuit that he was "going to get his money." The Citizen further reported he/she believed that Wilbern's son attended Fairport High School.

POST-LEAD INVESTIGATION

15. After receiving the information, law enforcement began to corroborate the lead. Law enforcement was able to confirm through Xerox Corporation that both the Citizen and Richard L. Wilbern were in fact employed by the Xerox Corporation at the same time. Wilbern was a full-time employee at Xerox with a hire date of August 11, 1997, although he began working there in September 1996 as a temporary hire. Wilbern's position was that of a copier/disassembler/cleaner/repairer/sander, sometimes referred to as a "scuffer." Wilbern worked in Building 200, just north of the XFCU location. Wilbern was terminated by Xerox on February 23, 2001 for repeated employment-related infractions. Xerox employment records from 2001 listed a home address of 120 West Avenue, Apt. 2, Fairport, New York.

16. Law enforcement was also able to confirm that on or about August 30, 2000, Wilbern did in fact bring a lawsuit against Xerox pursuant to Title VII of the Civil Rights Act alleging that Xerox unlawfully discriminated against him with respect to the terms and conditions of his employment, subjected him to a hostile work environment, failed to hire him for a position for which he applied because of his race, and retaliated against him for complaining about Xerox's discriminatory treatment. An amended complaint was filed on April 24, 2001, adding a retaliatory discharge claim. On or about December 12, 2002, pursuant to a motion for summary judgment filed by the Xerox Corporation, the Hon. Michael A. Telesca dismissed Wilbern's claims in their entirety. (00-CV-6431T).

17. Law enforcement was also able to determine that Richard Wilbern maintained checking and savings accounts at the Xerox Federal Credit Union. The defendant's paychecks were direct deposited into XFCU Account #XXXXXXX. Wilbern's 2001-2003 credit union statements list a home address of 120 West Avenue, Apt 2, Fairport, NY 14450. The accounts remained active and open as of August 12, 2003, the date of the robbery of the XFCU.

18. According to records obtained from Fairport High School, Wilbern's son, Rayard Akbar Wilbern, dob XX/XX/1986, was enrolled at Fairport High School during the 2000-2001, 2001-2002 and the 2002-2003 school year. Their records also indicate a reported address of 120 West Avenue, Apartment #2, Fairport, NY 14450.

PRIOR FELONY CONVICTIONS – PROHIBITED STATUS

19. Your affiant has conducted a criminal background check on Richard Wilbern. A review of Wilbern's criminal history showed that Wilbern was previously convicted for bank robbery. Specifically, Wilbern was arrested on September 3, 1980 in Irondequoit, New York and charged with Robbery 1st (armed with a deadly weapon) and Grand Larceny 2nd. The police report indicates that on September 3, 1980, Richard Wilbern entered the First National Bank of Rochester located at 1000 East Ridge Road, Irondequoit, New York armed with a handgun. Upon entering the bank, Wilbern pulled a stocking mask over his face and approached the manager. Wilbern handed the manager a bag and demanded it be filled. After obtaining United States Currency, Wilbern fled the bank and entered a waiting getaway vehicle being driven by a co-defendant. Shortly thereafter, the vehicle was pulled over and both Wilbern and his driver were arrested. Wilbern pled guilty to the felony of Attempted Robbery 2nd and served one year in jail.

20. Wilbern was also arrested on March 14, 1986, and charged with Possession of a Sawed-off Shot Gun and Carrying a Concealed Weapon in Richmond, Virginia. Further investigation determined that on May 20, 1989, Wilbern pled guilty to the felony level violations of Possession of a Sawed-off Shotgun and Possession of a Concealed Weapon. Wilbern was sentenced to 2 years and 30 days.

21. On January 7, 2004, just five months after the Xerox robbery/homicide, Wilbern was arrested in St. Clairsville, Ohio and charged with Receiving Stolen Property and Fictitious Vehicle Registration (stolen plates). A review of the incident report shows that a

replica toy gun was located in the vehicle operated by Wilbern. The defendant ultimately pled guilty to the original charge of Fictitious Vehicle Registration. The arrest booking photo shows Wilbern's height at 72", or 6' tall. (2004 photo attached hereto and made a part of this complaint as Exhibit A). Wilbern's height (6'0") matches the height analysis conducted by the Federal Bureau of Investigation Forensic Audio Video Image Analysis Unit. This is the also the same height listed on Wilbern's New York State driver's license.

DNA TESTING ON UMBRELLA

22. In the aftermath of the robbery/homicide at the Xerox Federal Credit Union, the Monroe County Public Safety Laboratory was called upon to obtain DNA samples from the green and gray umbrella which was left behind by the Subject. Two sets of swabs were taken from various locations on the umbrella, including the "external wrap around closure and button", the "lower latch mechanism", the "metal shaft and upper latch mechanism" and an "internal strap." One set of swabs was tested for the presence of DNA while the second set was allowed to dry, packaged and appropriately stored at the lab for future testing. Based upon the technology available at the time, while human DNA samples were located on the first set of swabs, there were insufficient amounts of DNA located in order to develop DNA profiles. Accordingly, at that time, no conclusions could be drawn.

23. On November 15, 2011, Webster Police investigators transferred the second set of swabs from the Monroe County Public Safety Building to the Office of Chief Medical Examiner (OCME) in New York City. OCME had developed the expertise and facilities

necessary to perform a DNA testing technique that enables testing to be performed on trace amounts of evidence. This testing technique is referred to as High Sensitivity DNA testing (also referred to as Low Template testing). On December 28, 2011, the Office of Chief Medical Examiner, New York City issued a report advising that they were able to recover Human DNA from each of the submitted swabs from the umbrella, and that two of the submitted swabs contained sufficient levels of Human DNA to conduct High Sensitivity PCR DNA testing and comparison. PCR testing, more formally called polymerase chain reaction (PCR) is a technique used in molecular biology to amplify a single copy or a few copies of a piece of DNA across several orders of magnitude, generating large amounts of DNA by repeated cycles of copying the DNA loci. As to Swab 8.2, which was taken from the "umbrella closure wrap around", the Medical Examiner concluded that DNA from at least two people was located, but included one major male contributor, referred to as "Male Donor A." The DNA profile of Male Donor A was a full profile, based on testing at 15 different loci positions. That DNA profile would be expected to be found in only 1 in 6.80 trillion people. The second sample, Swab 8.4, which was taken from the "umbrella latch mechanism (lower)" of the umbrella was also a significant profile, based on testing at 10 different loci positions. The DNA profile would be expected to be found in only 1 in 138 million people.

RICHARD WILBERN INITIATES CONTACT WITH THE FBI

24. A check with the records maintained by the FBI indicate that Richard Leon Wilbern made five calls to the FBI Public Access Line between July 14, 2015 and April 14, 2016. These complaints were apparently in relation to what he considered to be an unlawful foreclosure of his property at 766 Hudson Avenue, Rochester, New York. Wilbern claimed

to be the victim of a crime. The April 14, 2016 call to the FBI occurred just several weeks after the FBI press conference held on March 21, 2016.

25. On June 29, 2016, FBI agents contacted Richard Wilbern via the cell phone number he provided. Wilbern voluntarily agreed to come in to the FBI Office in Rochester on July 7, 2016, where he discussed the facts and circumstances of the fraud case with investigators. On July 19, 2016, Wilbern again agreed to come back to the FBI office to further discuss the fraud case. During that second meeting, Wilbern was asked to sign some paperwork and to seal the paperwork in an envelope, which he did by licking the envelope. Wilbern left the FBI offices after being advised that law enforcement would be in touch with him in the future. After observing Wilbern lick and seal the envelope, law enforcement immediately placed the envelope in a secured evidence bag for possible DNA testing and comparison.

DNA COMPARISON RESULTS IN POSITIVE MATCH TO RICHARD WILBERN

26. Shortly after obtaining the DNA sample from Richard Wilbern, the evidence was delivered to the Office of the Medical Examiner in New York City to be compared against the "Male Donor A" DNA profiles obtained from the umbrella in 2011. On September 1, 2016, law enforcement received the official report from the Office of the Medical Examiner. The Office of the Medical Examiner's report indicated that they were able to obtain a full DNA profile from the saliva contained on the envelope. As to Swab 8.2, which was taken from the "umbrella closure wrap around", the Medical Examiner's Office concluded that the DNA profile obtained from "Male Donor A" positively matched the DNA profile of the

sample obtained from Richard Wilbern. In other words, the DNA located on the "umbrella closure wrap around" is that of Richard Leon Wilbern. As stated above, the DNA profile of Male Donor A is expected to be found in only 1 in 6.80 trillion people. As for Swab 8.4, which was taken from the "umbrella latch mechanism (lower)", the Medical Examiner's Office concluded that DNA profile obtained from "Male Donor A" matches the DNA profile of the sample obtained from Richard Wilbern. As stated above, for Swab 8.4, the DNA profile of Male Donor A is expected to be found in 1 in 138 million people.

WILBERN'S AFFILIATION WITH AND SEARCH OF 23 TUBMAN WAY

27. On September 27, 2016, at approximately 2:17 p.m., the Hon. Jonathan W. Feldman issued a search warrant for the residence at 23 Tubman Way (garage only), Rochester, New York. According to records obtained by Rochester Gas and Electric, utility service at the location is in the name of Ferran Scott, Richard Wilbern's girlfriend. Upon searching the garage, agents discovered a large amount of men's clothing and other personal items belonging to Richard Leon Wilbern. Of particular relevance here, agents discovered the following items:

- a black, full face ski mask tucked inside a planner notebook;
- one (1) Feather Industries Inc. Model AT-9, 9 mm rifle, bearing serial number A91074, loaded with 25 rounds in the rifle magazine;
- one (1) Norinco SKS rifle, bearing serial number 24000873, loaded with 11 rounds of 7.62 x 39 caliber ammunition;
- one (1) SAA Model SA15 semi-automatic rifle, bearing serial number JT21474 along with two empty magazine clips;

- one (1) Kel Tec model Sub 2000, .40 Smith and Wesson caliber rifle bearing serial number EHZ06, along with 3 empty magazine clips, all located in a gun case.

28. As stated above, Richard Wilbern is a convicted felon and therefore precluded from possessing any firearms. On October 4, 2016, Ferran Scott was interviewed at the United States Attorney's office by your affiant. Scott stated that she has lived at the Tubman Street residence with her mother, Linda Mosely, and her two children. Both children are under the age of 7. She indicated that she and Richard Wilbern have been romantically involved for approximately 3 years. She indicated that she and Wilbern have one male child together. Scott stated that Wilbern travels a fair amount, but she believes that when he is present in Rochester, Wilbern stays with her at 23 Tubman Way. Scott stated that sometime in August 2016, Wilbern moved a number of personal items into her garage that Wilbern retrieved from a building he owned at 766 Hudson Avenue, Rochester, New York. She indicated that she permitted Wilbern to store those items in her garage. Scott further indicated she was not specifically aware of each of the items Wilbern brought and stored in her garage. She stated she was surprised to learn that there were firearms located in her garage, that they did not belong to her and that she would never have permitted loaded firearms to be kept in the house where her young children were present. That same day, your affiant also spoke with Scott's mother, Linda Mosely. Ms. Mosely stated that she was aware that Wilbern had some personal items stored in the garage, but indicated she had no idea that any guns were in the garage. Although Ms. Mosely indicated that she lawfully possesses two handguns (which are on her NYS pistol permit), she stated that none of the rifles inside the garage belonged to her. Lastly, both women indicated that no person other than Wilbern had any possessions stored in their garage.

GUN TRACES

29. On September 28, 2016, OST Kimberly K. Williams conducted a search through eJusticeNY's Stolen Gun database and submitted firearm trace requests through the ATF National Tracing Center for the four weapons that were seized pursuant to the execution of a search warrant at 23 Tubman Way, Rochester, New York.

a. Feather Industries Inc. Model AT-9, 9 mm rifle, bearing serial number A91074. eJusticeNY's Stolen gun was negative. ATF's firearms trace was completed on 9/30/2016. The firearm was purchased at Ray and Frank's Hunting Supplies on Stone Road in Greece, New York in 1990. The owner of the firearm indicated that the gun was stolen approximately 11 years ago. The theft was never reported to the police.

b. Norinco SKS rifle, bearing serial number 24000873. eJusticeNY's Stolen gun was negative. This firearm was unable to be traced.

c. SAA Model SA15 semi-automatic rifle, bearing serial number JT21474. eJusticeNY's Stolen gun was negative. ATF's firearms trace was completed on 9/30/2016. The firearm was purchased from Katy Gun Gear in Katy, Texas in March 2016. The gun was sold privately at a gun show in Texas in 2016. No report or record of purchaser.

d. Kel Tec model Sub 2000, .40 Smith and Wesson caliber rifle bearing serial number EHZ06. eJusticeNY's Stolen gun was negative. ATF's firearms trace was completed on 10/7/2016. The firearm was purchased in 2013 from American Firearms in Katy, Texas. The gun was sold privately at a gun show in Texas in 2016. No report or record of purchaser.

ARREST OF RICHARD WILBERN AND SEIZURE OF AN APPLE iPHONE

30. On September 27, 2016, Richard L. Wilbern was arrested pursuant to a criminal complaint charging him with violations of Title 18, United States Code, Sections 2113(a), 2113(e) and 2 (credit union robbery, resulting in death), and that he committed a violation of Title 18, United States Code, Sections 924(c)(1)(A)(iii) and (j)(1) (possession and discharge of a firearm in furtherance of a crime of violence, resulting in death). Subsequently, he was charged in a separate complaint with unlawful possession of firearms by a prohibited person (convicted felon) pursuant to Title 18, United States Code, Section 922(g). On or about February 15, 2017, Wilbern was detained after a bail hearing held pursuant to Title 18, United States Code, Section 3142(f).

31. Incident to the defendant's arrest, law enforcement seized an Apple iPhone from the person of Richard Wilbern, more particularly described as one (1) **Apple Iphone 6S Plus, Model A1687, FCC ID BCG-E2944A.** In or about June 2017, your affiant applied to this Court under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the seized iPhone. Your affiant was advised at that time that certain capabilities had been developed and were being offered through the F.B.I. to open the otherwise password-protected Apple device. Several extensions of the search warrant have been granted, the latest of which was signed by the Hon. Jonathan W. Feldman on or about November 16, 2017, extending the time in which to complete the search until December 19, 2017. However, notwithstanding best efforts, at the time of this submission, agents with the FBI have not been able to access the contents of the cellular phone.

32. As I articulated in my original application to search the Apple Iphone 6S Plus, Model A1687, FCC ID BCG-E2944A, I am aware, based upon my training and experience, that:

(a) Individuals involved in criminal activity commonly maintain names, telephone numbers, recorded messages, photographs, letters, cables, telegrams, personal notes and other items of information concerning themselves and individuals associated in their criminal activities, in electronic storage mediums, including but not limited to cellular telephones and computer devices;

(b) Individuals involved in criminal activity commonly take, or cause to be taken, photographs/videos of themselves, their associates and their property. These photographs/videos are usually maintained in their residences and/or stored in electronic storage mediums, including but not limited to cellular camera telephones and computer devices.

(c) Individuals maintain written documents, letters, diaries, notes, email communications, text communications, and other records in their personal computers.

(d) Individuals access the internet and may download files or other media content onto their personal computers.

33. During the course of my career, I have had the opportunity to assist with the execution of several federal search warrants on cellular telephones and computer hard drives seized from members of criminal organizations which have resulted in the recovery of significant evidence tending to show involvement in criminal activity. Based on the evidence in this investigation, your Affiant has probable cause to believe that relevant and material messages, call logs, notes, emails, photographs, contacts and other information may be stored in the iCloud connected to Wilbern's Apple ID. Despite efforts to unlock the iPhone pursuant to the aforementioned search warrant, it is believed that data which is maintained on the iPhone (along with other evidence relevant to the investigation) may have been

uploaded, synced and stored in the iCloud account associated with Wilbern's Apple ID. Specifically, I believe that there is reasonable cause to believe that evidence of the Xerox crime, including the identity of potential co-conspirators, may be maintained in electronic format. Moreover, with respect to the charge of Title 18, United States Code, Section 922(g), the government will be required to prove at trial that the defendant "possessed" the firearms listed above, notwithstanding the fact they were not in his actual possession at the time they were seized.

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

34. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

35. Apple provides a variety of services that can be accessed from Apple devices, including the iPhone, iPad, and iPod Touch, or in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

---

1 The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, backup and synchronize data on Apple devices, including the iPhone, iPad, and iPod Touch or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

36. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

37. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user

accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

38. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

39. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

40. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

41. Most importantly, as it relates to the facts of this case, Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages,

voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

42. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In this case, I believe that there is reasonable cause to believe that evidence of the Xerox crime, including the identity of potential co-conspirators, may be maintained in electronic format. Moreover, with respect to the charge of Title 18, United States Code, Section 922(g), the government will be required to prove at trial that the defendant "possessed" the firearms listed above, notwithstanding the fact they were not in his actual possession at the time they were seized. The government believes that information maintained by Apple, and more particularly stored on the iCloud services, may provide additional details, including call logs, notes or photographs, providing information as to how and when the firearms were acquired by the defendant.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

44. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant.

46. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)

and (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Andrew Jasie, NYSP
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed to before me
this 29 day of November 2017.

HON. JONATHAN W. FELDMAN
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with APPLE ID **richwilbern@gmail.com** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Apple

To the extent that the information described Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit

Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken;

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be Seized by the Government

All information described above in Section I that constitutes contains records, fruits, instrumentalities, and evidence of a crime, or tending to demonstrate personal involvement or knowledge of the crime of Title 18, United States Code, Sections 2113(a), 2113(e) and 2 (credit union robbery, resulting in death), and a violation of Title 18, United States Code, Sections 924(c)(1)(A)(iii) and (j)(1) (possession and discharge of a firearm in furtherance of a crime of violence, resulting in death), and/or the unlawful purchase or acquisition of firearms by a prohibited person, in violation of Title 18, United States Code, Section 922(g), for each account or identifier listed on Attachment A.

a. The identity of the person(s) who created or used the Apple ID.

b. Evidence indicating how and when the account was established, accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation;

e. Evidence that may identify any co-conspirators or aiders and abettors, or others with personal knowledge of the crimes under investigation.

f. Evidence related to the identification of all persons involved in the acquisition or transfer of certain firearms found in the possession of Richard Wilbern in or about September 2016.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature